

**WEEK - 6**

**Computer Networks**

**M. Sumanth Reddy**

**Intro:**

Wireshark is a popular open-source network protocol analyzer used for network troubleshooting, analysis, software and communication protocol development, and education. It allows users to capture and inspect the data traveling back and forth on a network in real-time. Wireshark supports a wide range of network protocols and can be used on various platforms, including Windows, macOS, and Linux.

Which we can do with Wireshark is:

* Packet Capture and Analysis
* Protocol Support
* Live Capture and Offline Analysis
* Display Filters
* Graphical User Interface (GUI)
* Color-coded Packet Display
* Statistics and Graphs

**Wireshark Tutorial 1: Changing the Column Display**

In the first tutorial we will learn about:

* Wireshark Version Check
* Configuration Profiles
* Web Traffic and the Default Wireshark Column Display
* Change Date and Time
* Customized columns
* Hiding Columns
* Exporting Your Updated Configuration Profiles

**Wireshark Version Check:**

For every device we use there is a version, in the same way there is also version of the software we use. So, to check the version the Wireshark, open the Wireshark on the top we can see the different option click on the help and select About Wireshark and displays the version and some information about Wireshark.

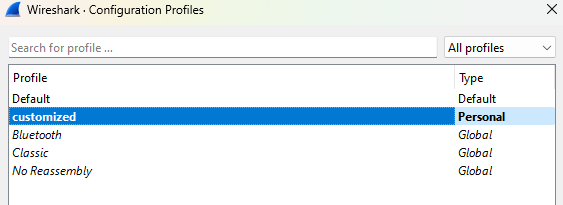


**Configuration Profile:**

After checking the version, now we configure profiles through

Go to edit option and select Configuration Profiles and re-enter the **Default** into the **customized** and type as Personal.

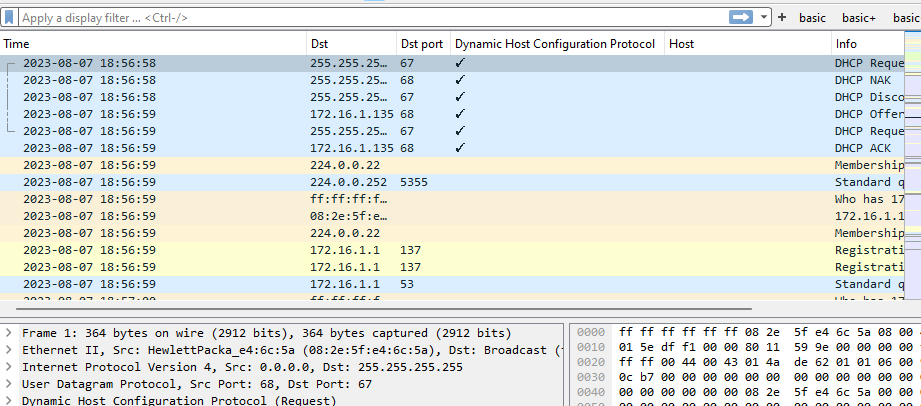
When we change it, if we are working on any other file in wireshark it will be saved as customized to store the newly created profile.



**Web Traffic and Default Wireshark Column Display:**

In the Wireshark’s column it provides a view of web traffic in the data wise in the default way.

And we can also add, delete or interchange the columns between them as per our convenience.



The upper picture contains different types of data:

**Time**: Seconds broken down to the microsecond from the first frame of the pcap. The first frame is always 0.00000

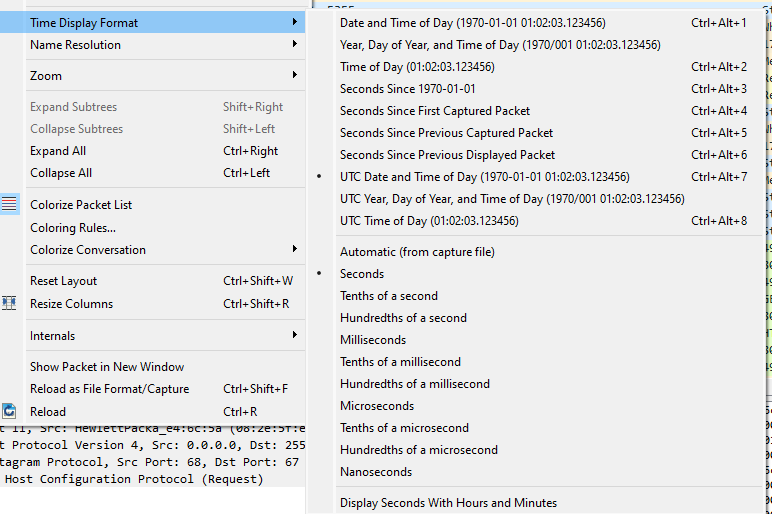
**Destination:** Destination address, commonly an IPV4, IPV6 or Ethernet address

**Info:** Information about the Ethernet frame, IP Packet or TCP segment.

**Change Data and Time:**

We can also change Date and Time, Seconds since first captured or Seconds since previous captured and many more...

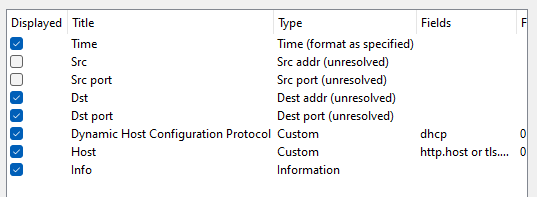
From select View -> Time Display Format...



**Adding columns:**

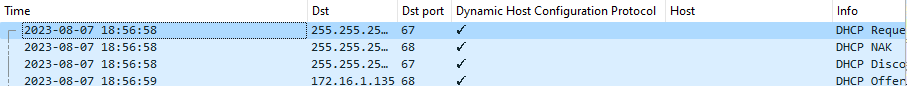
we can also do many operations on the columns like Adding new columns, Removing columns and customization of columns.

To add the columns, click right click on the any column and select column preferences and it open a new tab, there we can see **[ + ]** symbol which used to add column.



And we can also check or uncheck them for their work in the traffic.

Which was selected above will be displayed on the columns.



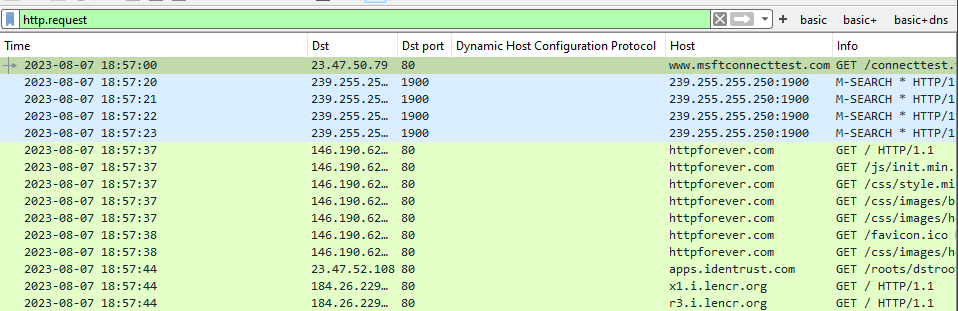
**Customized Columns:**

Wireshark also allows users to add customized columns based on almost any value found in the frame details window.

There is a display filter, and we can enter any filter. **http.request**

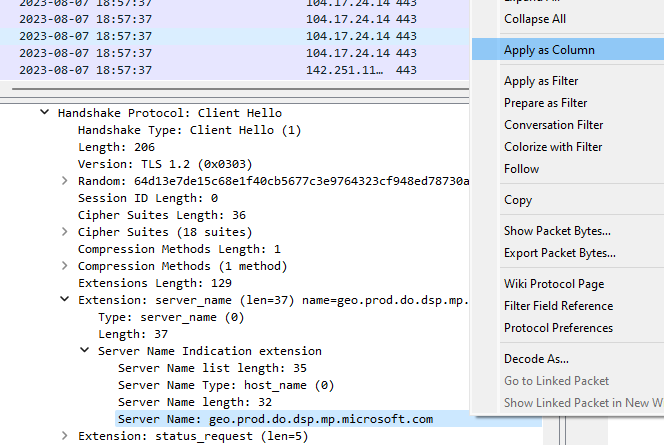
If it turns **red,** it is invalid

If it been **green**, it is valid.

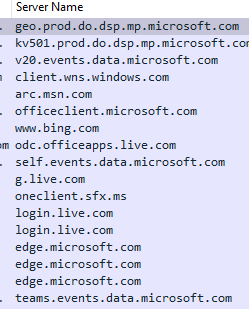


And there are many customized columns for domains used in encrypted HTTPS web traffic.

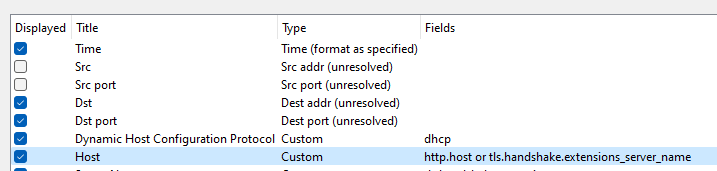
Type **tls.handshake.type eq 1** on the display filter and add column of Server name as shown in the picture below.



After adding the column, Server Name will be added to traffic list.



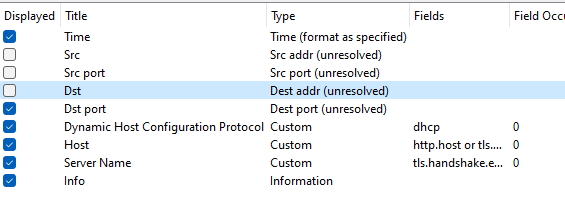
To save screen space, we should combine these two columns into a single column using **or** function. First, double-click on the Fields value in the Server Name entry and copy the text reading **tls.handshake.extensions\_server\_name**



**Hiding Columns:**

We can also HIDE the columns by unchecking them in column preferences. Because of the web traffic generated by the malware.

The Unchecked columns will not be visible in the Web traffic lists.

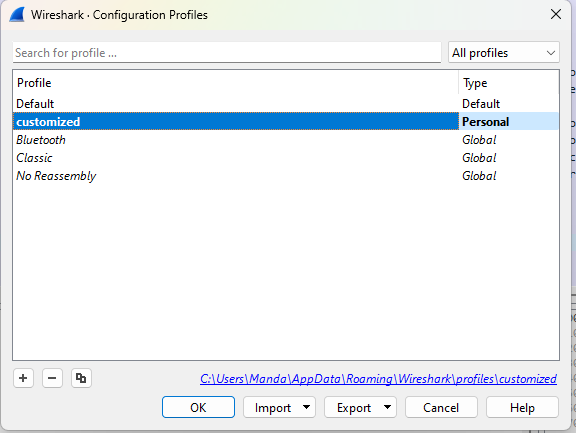


**Export the Updated Configuration Profile:**

After finishing the changes in the Traffic, we can Export them into a folder using a file name.

This is useful when installing wireshark in a new environment. To export click on the Edit and select the configure the profiles and click on the **Export,** select the folder and enter filename.

Save the file in: ZIP FILE



Conclusion: In the first tutorial we learnt about configuring the profiles and adding and deleting the columns and helps in the find the protocol easily in the traffic by entering their name, and we can choose what must be display and what to not.

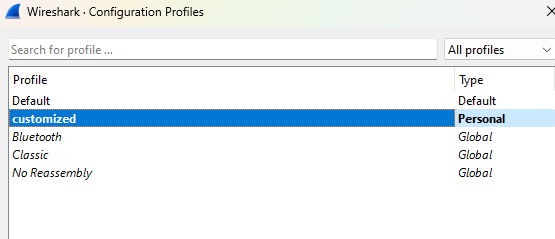
**Wireshark Tutorial 2: Display Filter Expressions**

In the second tutorial we will learn about:

* Wireshark-tutorial-filter-expressions-1-of-5.pcap
* Wireshark-tutorial-filter-expressions-2-of-5.pcap
* Wireshark-tutorial-filter-expressions-3-of-5.pcap
* Wireshark-tutorial-filter-expressions-4-of-5.pcap
* Wireshark-tutorial-filter-expressions-5-of-5.pcap

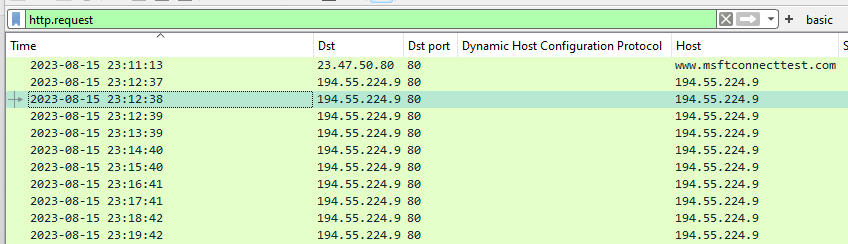
**Wireshark-tutorial-filter-expressions-1-of-****5.pcap:**

While using the Wireshark filter to ensure you are using personal profile, check the right side of the status bar, which shows the name of your current profile. You can also select “Configuration Profiles…” under the Edit menu to verify. Both options are shown below



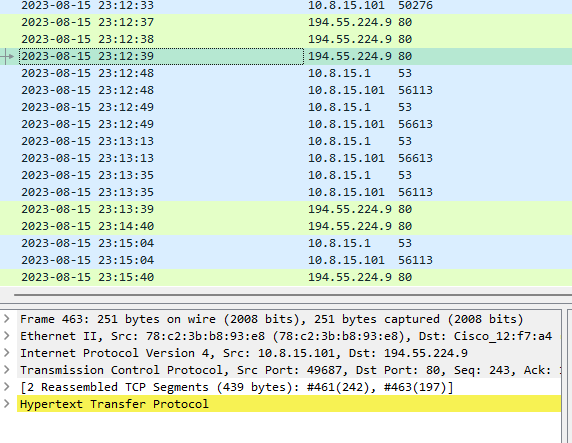
**The Wireshark Display Filter:**

In Wireshark's default configuration, the display filter is a bar located immediately above the column display. This is where we type expressions to filter our view of Ethernet frames, IP packets or TCP segments from a pcap



We can also search in display filter using **&&**(and) and **||**(or) functions.

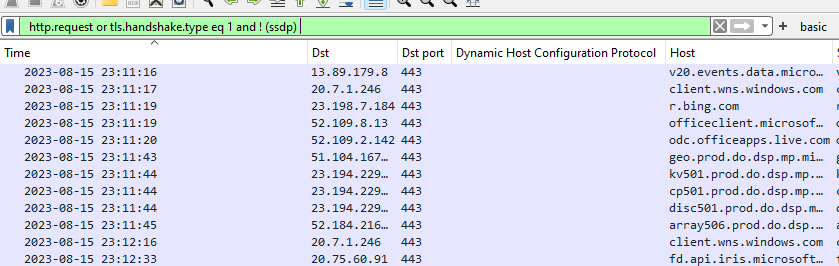
The green result displays the HTTP request lines.



**Filtering for Web Traffic:**

In Wireshark we can filter by the expressions **http.request or tls.handshake.type eq 1 and ! (ssdp)**

Shows the domain names used in HTTPS or SSL/TLS traffic and we can exclude SSDP traffic in our results.

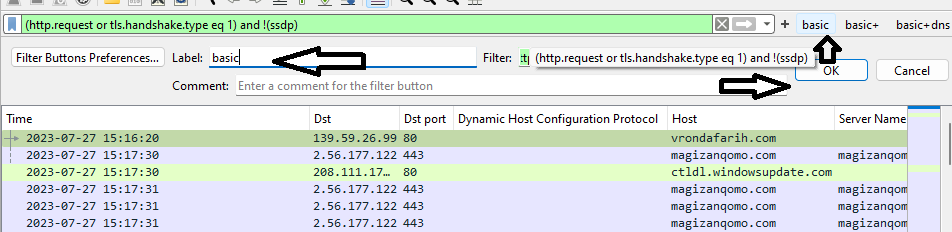


**Wireshark-tutorial-filter-expressions-2-of-****5.pcap:**

Our second pcap Wireshark-tutorial-filter-2-of-5.

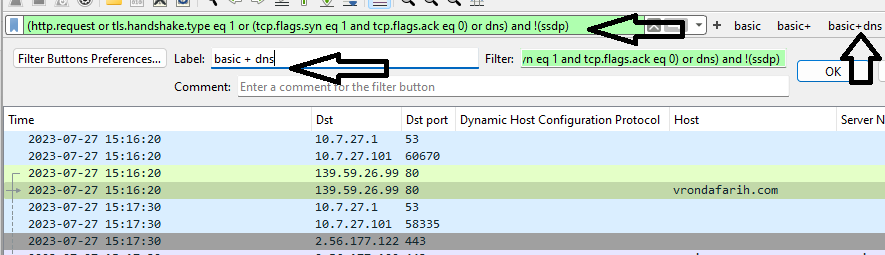
**Creating Filtering Buttons**

We can filter using the basic web filters. To ensure that filter is working click on [ + ] beside the display filter. And add **basic** in Label and click on **OK**



|  |  |
| --- | --- |
| basic | basic (http.request or tls.handshake.type eq 1) and !(ssdp) |
| basic+ | basic (http.request or tls.handshake.type eq 1 or (tcp.flags.syn eq 1 and tcp.flags.ack eq 0)) and !(ssdp) |
| basic+dns | basic (http.request or tls.handshake.type eq 1 or (tcp.flags.syn eq 1 and tcp.flags.ack eq 0) or dns) and !(ssdp) |

Using this we can do many operations in the Display filter

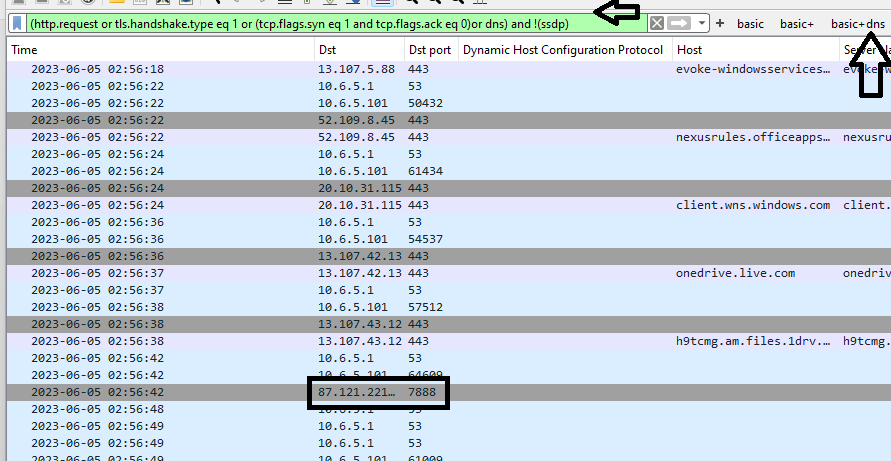


**Wireshark-tutorial-filter-expressions-3-of-****5.pcap:**

Our third pcap Wireshark-tutorial-filter-3-of-5.

**Filtering for Non-Web Traffic:**

This pcap contains post-infection traffic generated by a Remote Access Tool (RAT) malware called Ave Maria RAT.



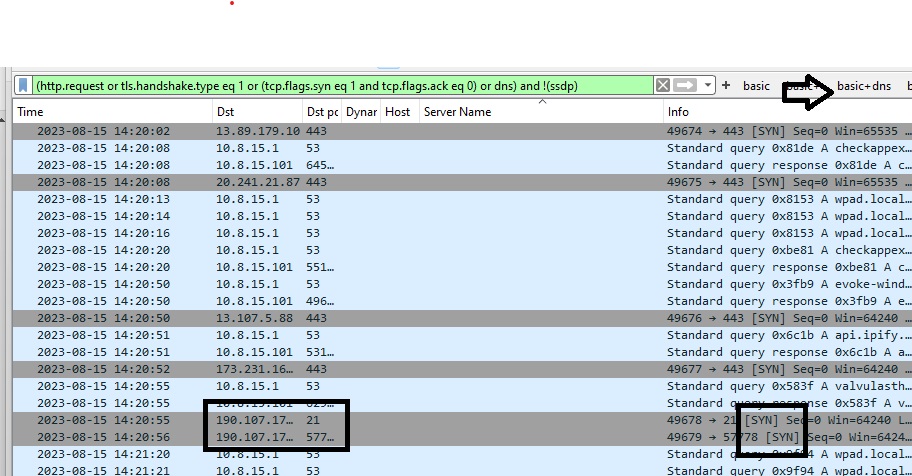
We can find a DNS query for adaisreal.ddns[.]net that resolves to 87.121.221[.]212, then a TCP segment to that IP address with the SYN flag over TCP port 7888.

**Wireshark-tutorial-filter-expressions-4-of-****5.pcap:**

Our fourth pcap Wireshark-tutorial-filter-4-of-5.

**Filtering for FTP Traffic:**

This contains post-infection activity caused by a malware executable that generates FTP traffic. Our **basic+dns** filter reveals traffic over TCP port 21 and another TCP port after a DNS query to valvulasthermovalve.



Our “basic+dns” filter can help find unencrypted FTP traffic, but other filter expressions would better fit an FTP search. Two basic Wireshark filters for unencrypted FTP traffic.

**Ftp: FTP activity in the control channel (TCP port 21)**

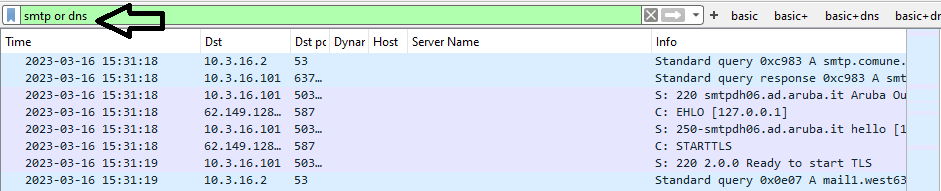
**Ftp-data: FTP activity in the data channel (ephemeral TCP port)**

**Wireshark-tutorial-filter-expressions-5-of-****5.pcap:**

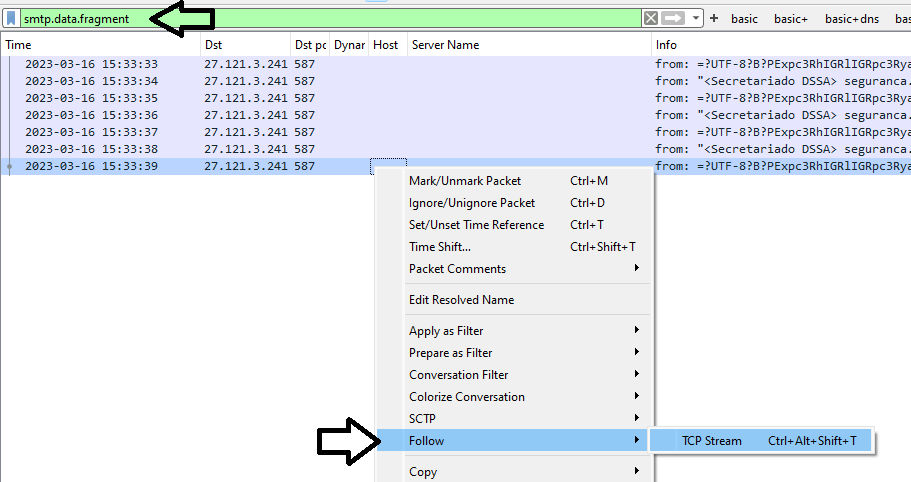
Our fifth pcap Wireshark-tutorial-filter-5-of-5.

**Filtering for Email (Spambot) Traffic:**

In addition to FTP, malware can use other common protocols for malicious traffic. Spambot malware can turn an infected host into a spambot designed to constantly send email messages. This is characterized by a large amount of DNS requests to various mail servers followed by SMTP traffic on TCP ports 25, 465, 587 and other ports less-commonly associated with SMTP traffic.



Now we will type **smtp.data.fragment** and right click on any Dst and select Follow and Select TCP stream.



After doing above operation, we will get the output as below:

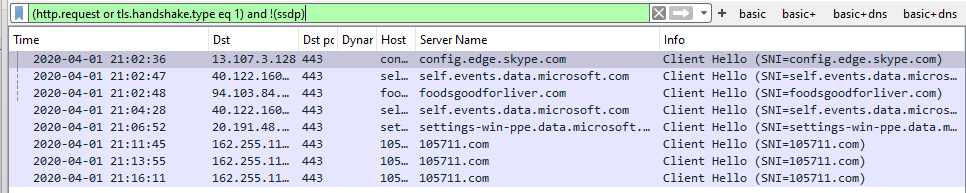


**Wireshark Tutorial 3: Display Filter Expressions**

The third tutorial is about **HTTPS Traffic Without the Key Log File.** We use

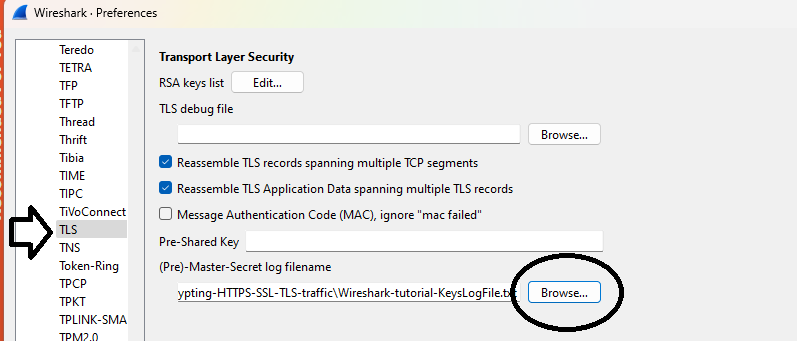
(http.request or tls.handshake.type eq 1) and! (ssdp)

Now type the above commands in the display filter.



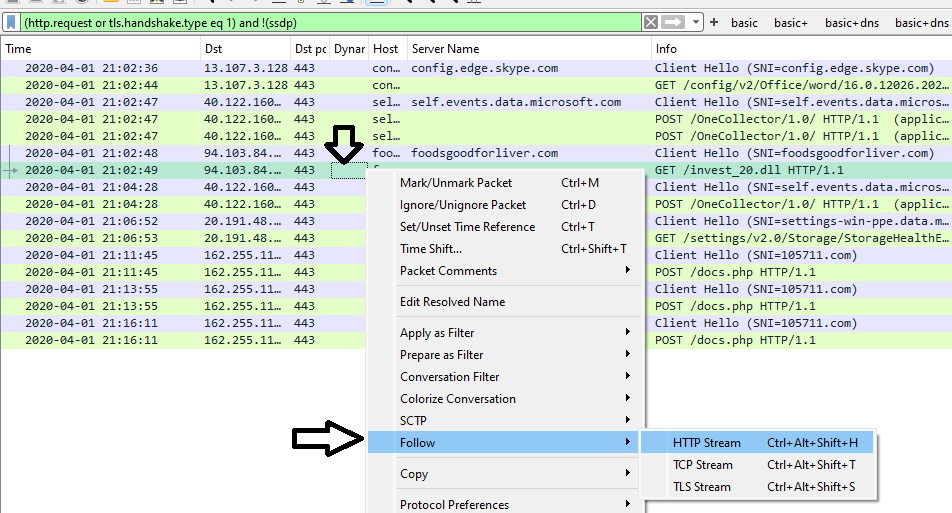
**Loading the Key Log file:**

Open **Wireshark-tutorial-on-decrypting*-*HTTPS-SSL-TLS-traffic.pca*p*** in Wireshark. Then use the menu path **Edit --> Preferences --> Protocols to** bring up the Preferences. And select the TLS...

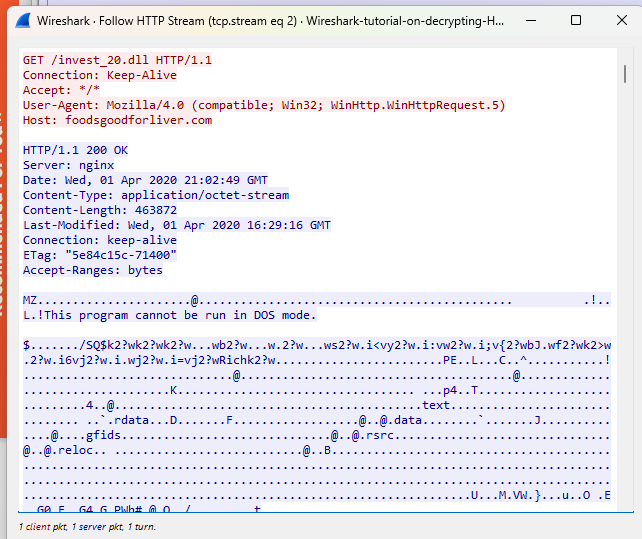
After that click on the Browse and select the Wireshark-tutorial-KeyLogFile.txt and hit the OK button.

**HTTPS Traffic with the Key Log File:**

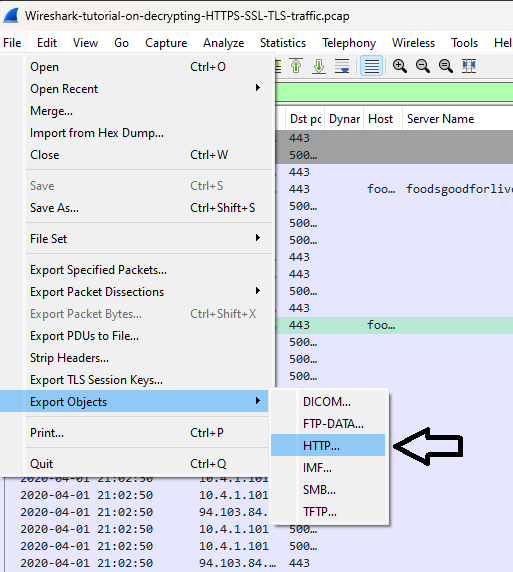
Once you click on the “OK”, when using the basic filter, Wireshark column will display the list contains of decrypted HTTP requests under the each of the HTTPS.



Then right click on the foodsgoodforliver[.]com - GET /invest\_20.dll and select the HTTP Stream as in the image. Then it displays the...



Since we have the key log file for this traffic, we can now export this malware from the pcap. Use the menu path **File --> Export Objects --> HTTP** to export this file from the pcap.



After Click on HTTP a window will pop up then select the **632 foodsgoodforliver.com** and save it.

